REMARKS

In the Official Action mailed 6 October 2004, the Examiner objected to the Abstract as being too lengthy. The Examiner reviewed claims 1-55. The Examiner rejected claims 1-11 and 45-55 under 35 U.S.C. §101; rejected claims 12-15, 22-26 and 34-37 under 35 U.S.C. §103(a); and rejected claims 16-23, 27-33 and 35-44 under 35 U.S.C. §103(a).

Applicant has amended the Abstract; and amended claims 1, 5, 7, 11, 12, 16, 18, 22, 23, 34, 45, 49, 51 and 55 as explained below, or to correct typographical errors. Claims 1-55 remain pending.

The Examiner's objection and rejections are respectfully traversed below.

Objection to the Abstract

The Examiner objected to the Abstract, because it was too long. Applicant presents an amended Abstract herein. Accordingly, reconsideration of the objection is requested in view of the amended Abstract.

Rejection of Claims 1-11 and 45-55 under 35 U.S.C. §101

Claims 1-11 and 45-55 are rejected under 35 U.S.C. §101 as non-statutory. Although the Examiner did not expressly reject claim 12, the Examiner suggested amendment of it in the discussion. Applicant has amended independent claims 1, 12 and 45, without loss of scope, to recite technological features inherent in the data processing methods recited, and made conforming amendments to other claims. In particular, claims 1, 5, 7, 11, 12, 16, 18, 22, 45, 49, 51 and 55 have been amended to explicitly recite processing steps that are executed using a computer-based data processing system. Thus, such claims are statutory subject matter under the analysis of *Ex Parte Bowman*, 61 USPQ2d 1669 (Bd. Pat. App. & Inter. 2001) (cited by the Examiner), and *AT&T Corp. v. Excel Communs., Inc.*, 172 F.3d 1352, (CAFC, 1999).

Accordingly, reconsideration of the rejection of claims 1-11 and 45-55 as amended is respectfully requested.

Rejection of Claims 12-15, 22-26 and 34-37 under 35 U.S.C. §103(a)

Claims 12-15, 22-26 and 34-37 are rejected under 35 U.S.C. §103(a) as being unpatentable over (US 6,098,053) Slater in view of (US 5,991,750) Watson. For the purpose of

discussion, we point out that independent claims 12, 23 and 34 include an "authentication" element, and "authorization" element, and an "accounting" element.

In connection with the authentication element of the claims, the Examiner takes the position, mistakenly, that Slater (col. 1, lines 55-67, col. 2, lines 19-31, and col. 4, lines 31-65) teaches the step of "executing an authentication process... for a predicted transaction by a particular account holder" as recited in claim 12, and a process of "authenticating a predicted transaction by a particular account holder," as recited in claim 34. We note that the Examiner did not explicitly mention independent claim 23. At the first citation to Slater, at col. 1, lines 55-67, Slater describes a point of sale transaction that uses the automated teller machine network, and processes used for routing the transaction in the network. The authentication for the point of sale transaction comprises possession of "their ATM, debit or check card" for swiping, and entry of a personal identification number PIN. The PIN and possession of the card in Slater are transaction independent. There is no authentication of a "predicted transaction," as required in claim 12, in claim 23 and in claim 34. There is no mention of a "transaction signature," as required in claim 12, in claim 23 and in claim 34. Likewise, there is no mention of storing of a "transaction signature and parameters associated with predicted transaction," as required in claim 12, in claim 23 and in claim 34.

At the second citation to Slater, at col. 2, lines 19-31, Slater describes the benefit of an ATM/POS transaction, in terms of cost savings for both the purchaser in the merchant. The citation is unrelated to authentication.

At the third citation to Slater, at col. 4, lines 31-65, Slater describes a transaction in which "purchaser payment instructions" are created, and securely communicated by encryption or digital signature. Thus the authentication involved in the transaction described at this third citation involves possession of the card, a personal identification number, as well as potentially a digital signature for use with encryption. The PIN, digital signature, and possession of the card in Slater are transaction independent. A digital signature provides no authentication of a card holder but just insures data integrity while in transit. Moreover, according to Slater, at col. 8, lines 12-16, symmetric encryption keys at the card reader and the financial institution back office are preset and, therefore, they are not transaction specific keys, which jeopardizes the security of the digital signature against intruder attacks and of the encrypted data as well. There is no authentication of a "predicted transaction by a particular account holder," as required in claim 12

and in claim 34. There is no mention of a "transaction signature," as required in claim 12 and in claim 34. Likewise, there is no mention of storing of a "transaction signature and parameters associated with predicted transaction," as required in claim 12 and in claim 34.

Turning to the authorization element of the claims, the Examiner cites Slater at col. 5, lines 2-25. At this citation, Slater describes reformatting encrypted financial transaction instructions into a form accepted by the on-line ATM/POS transaction system. This reformatting does not appear to be related to authorization of a transaction as required in claim 12 and in claim 34. Next, Slater states that the purchaser's bank issues a message of approval in response, thereby authorizing a transaction, "if the financial transaction is acceptable." (Slater, col. 5, line 13). There is no discussion of how the authorization process works in this citation. Thus, the citation by the Examiner does not teach use of a "transaction signature" that is produced during an authentication process, as required in claims 12, 23 and 34. Slater does not teach a process requiring matching of an entered transaction signature with a transaction signature generated during authentication of a predicted transaction, matching of predicted and actual transaction amounts, and that the actual transaction time needs a time criterion, as required in claims 12 and 34.

Turning finally to the accounting element of the claims, the Examiner acknowledges that Slater does not apply. Rather, the Examiner applies Watson to suggest this element. In particular, the Examiner cited Watson at col. 8, lines 31-64. At this section of Watson, a description of setting up special-purpose accounts is described. This has nothing to do with the accounting element of claims 12, 23 and 34. In particular, Watson does not describe reconciling a predicted transaction amount with an actual transaction amount, as required in claims 12, 23 and 34.

Embodiments of the present invention address the security and privacy of a financial account holder in credit or debit card, online and offline financial transactions, and introduce a major shift in basic transaction architecture and back office technology for large volumes of transactions and accounts. Unlike conventional financial transaction architectures, where a card holder authentication is hardly present and is technologically weak, being implicit in possession of a card, and occasionally of a PIN, embodiments described in the present application enable and enforce an authentication stage of a financial transaction which is performed first by the account holder in a communication session with the financial institution back office, where the

account resides, and typically separate from any interaction with a merchant (see Figs. 3-5 of the present application). Further enhancing this architecture, the authentication stage is associated with predicted financial transaction timing, security, and accounting parameters and automated at the financial institution back office to sustain mass user transactions.

In described embodiments, if the authentication stage of a financial transaction is successful, the card holder obtains from the back office a transaction signature which is transaction specific, as it points to a certain transaction time and projected transaction amount.

The Examiner's reliance on Slater and Watson is misplaced, as both patents address different objectives in totally different financial transaction architectures. Slater's key idea is to use an ATM/POS network to enable access to checking or saving accounts for completing a conventional ATM, debit, or smart card financial transaction (Slater, Fig. 1), as it is cheaper for a purchaser and a merchant as compared to conventional networks used for credit cards (like VISA). Slater centers his description around the network routing and security on communication lines, whereas Slater's financial transaction architecture remains a conventional one, in which a card holder submits a purchasing request to a merchant, and the merchant requests authorization from respective financial institutions. Certainly, the merchant is still empowered to request the card holder's signature and/or identification documents during offline transactions, or request entry of personal and private verifiable information during online transactions, to assure the card holder's authenticity. The architecture described and claimed herein allows eliminating this stage of providing personal and private verifiable information for review by the merchant to authenticate the card holder. Rather, the present invention introduces card holder transaction security and privacy by enabling the card holder with only a transaction signature and an account number to perform a financial transaction without the need to disclose personal information for authentication. Transaction security is enhanced in the architecture described and claimed herein, because (i) card holders go through a standard strong authentication gateway at the financial institution back office where the accounts are residing and where this private and personal information is protected (ii) card holders' private and personal information is not disseminated at multiple merchant offline and online entry points where it is collected by merchants and then misused and/or sold for profit, or becomes prone to network intruders (or intruding organizations) stealing this information at the multiple network access points or merchant databases.

Like Slater, Watson's patent remains within the framework of conventional financial transaction architectures (Watson, Fig. 2A). The Watson invention is focused on amending the authorization stage of a financial transaction in a way which would allow an account manager to pre-authorize certain transactions by superimposing on these transactions specific transaction identifiers set up by an account manager during an account set up. Neither Watson nor Slater introduces, discusses, or considers an authentication stage of a financial transaction, which, along with a combination of other transaction stages, recited in the claims herein, allows for a card holder to perform the transaction without disclosing the card holder's private and personal information to a merchant. Further, embodiments described herein address needs for a specific infrastructure to handle the newly provided financial transaction architecture at a financial institution back office, including clocked authentication, authorization, and accounting methods to enable mass user transactions.

In connection with claims 13 and 24, which depend from claims 12 and 23, respectively, and recite that the transaction signature is stored associated with a predicted transaction in a database, the Examiner relies upon Watson at col. 10, lines 35-57 and col. 11, lines 37-49. In these citations, Watson describes storing a quote amount, a variance, a merchant ID, an acquiring bank identification number, and the like, which are entered by an account manager as a pre-authorizing agent for ANY financial transaction initiated eventually by the card holder, whereas in embodiments of the present invention, the transaction signature is generated during authentication for a PARTICULAR financial transaction. The crucial difference here is that Watson's parameters stored in the database work for an unspecified number of future financial transactions, and are matched with information stored at account set up, whereas the claimed transaction signature relates to a predicted transaction, for which the parameters relating to a predicted amount and a time are provided by a card holder.

In connection with claims 14, 25 and 36, which depend from claims 12, 23 and 34, respectively, the Examiner relies on Watson to suggest "storing a parameter indicating acceptable transaction times in the database." The Examiner relies on Watson at col. 11, line 58 to col. 12, line 15, to support the rejection. However, the Examiner is mistaken. Watson does not describe the process of storing a parameter indicating acceptable transaction time. The Watson process does not generate a transaction signature for a predicted transaction. Rather, the account in Watson is set up in a manner that works with any number of future transactions.

Since the administrator can not anticipate when and how many future transactions are going to be initiated by the card holder, there is no information stored in the database concerning transaction times as required in claims 14, 25 and 36.

In connection with claims 15, 26 and 37, which depend from claims 12, 23 and 34, respectively, the Examiner relies upon Slater at col. 10, lines 32-49 and col. 10, lines 59-67. These claims require setting up a time out interval between the authentication time and the authorization time. Analysis of Slater reveals that it does not describe such a process. The time interval described at column 10, lines 62-67 of Slater relates to timing between authorization and execution of the purchase. This is not related to the time between authentication and authorization as required in these claims.

The Examiner did not explicitly address claim 22 in the analysis. Such claim depends from claims 12, and is allowable for at least the same reasons, and because of the unique combination recited.

Accordingly, reconsideration of the rejection of claims 12-15, 22-26 and 34-37 is respectfully requested.

Rejection of Claims 16-23, 27-33 and 35-44 under 35 U.S.C. §103(a)

Claims 16-23, 27-33 and 35-44 are rejected under 35 U.S.C. §103(a) as being unpatentable over Slater and Watson in view of (US 6,178,409) Weber et al., hereafter Weber.

Claims 16-22 depend from claim 12, claims 27-33 depend from claim 23 and claims 35-44 depend from claim 34, as discussed in detail above. Such claims are believed allowable for at least the same reasons as their respective base claims, and because of the unique combinations recited. We note that the Examiner includes claim 23 in this list as well as in the set of claims rejected without reliance on Weber. It is submitted that Weber does not overcome the deficiencies of Slater and Watson, and that claim 23 is allowable for the reasons discussed above.

Weber considers conventional transaction architecture within the frame of e-commerce when a customer makes an online purchasing request to a merchant which uses a special online service (a payment gateway) to connect to the financial institution back office for the payment authorization (Weber, Fig. 1B, col. 12, line 63 – col. 13, line 5, and col.17, lines 55-63). Unlike embodiments of the present invention, where the card holder's authentication stage provides a

transaction signature for a predicted transaction, provided the authentication is successful and the predicted transaction parameters are accepted, Weber does not have any explicit card holder's authentication stage and does not have a transaction signature as claimed herein.

The Examiner relies on Weber (col. 14, lines 12-15 and lines 58-67, and col. 15, lines 1-10) to suggest language from claims 16, 17 and 38, like the following quote of part of claim 16:

"The method of claim 12, wherein the authentication process includes:

establishing a private communication session between the particular account holder and a financial transaction server;"

However, the Examiner's citations to Weber do not describe the claimed authentication process that further includes establishing a private communication session between the particular account holder and a financial transaction server. Weber describes a transaction architecture in which a card holder establishes an online communication session with the merchant, submitting the card holder's purchasing request, which is subsequently reformatted and readdressed to a financial institution back office for an authorization request. The session with the merchant may include authentication by a certificate as described at col. 14, lines 12-47. However, the authentication suggested in Weber does not result in producing a transaction signature as claimed, and is otherwise unlike the claimed authentication process. The sections of Weber at col. 12, lines 58-67 and col. 15, lines 1-10, do not describe authentication.

In connection with the limitation in claims 16 and 38 that an account number and an identification number be accepted at the server during the authentication process, the Examiner cites Weber at col. 15, line 63 to col. 16, line 12. However, this section of Weber is related to a payment authorization request by the merchant, not authentication for a predicted transaction as required in the present claims.

In connection with the limitation in claims 16 and 38 that a predicted transaction amount be received at the server, the Examiner cites Weber at col. 24, lines 7-56, Fig. 1, Fig. 7B, and Fig. 15A. Again, however, these citations are not related to authentication. Rather they relate to a payment transaction in which actual funds are transferred. There is no "predicted" amount used in an authentication process described by Weber.

In connection with the limitation in claims 16 and 38 that a transaction signature be generated and identifying information be stored at the server, the Examiner cites col. 42, line 30 – col. 47, line 41, col. 64, lines 30-57, Fig. 1A, Fig. 15B, and Fig. 17. Applicant submits that the Examiner is mistaken. Applicant's review of Weber suggests that there is no transaction signature generated in an authentication process, based on a predicted transaction, as required in the claims present here. This might be understood with reference to Fig. 17 of Weber, which begins with a sales order for an actual transaction from a customer.

Claim 17 depends from claim 16, and is allowable for at least the same reasons, and because none of the references suggest the claimed prompting in the context of authentication. Perhaps this is a typographic error, and the Examiner intended to refer to claim 27. Claim 27 includes limitations like those discussed above in connection with claims 16 and 38, and is allowable for at least the same reasons.

In addition, the Examiner's argument that persons of skill would be motivated to combine the teaching Weber with Slater and Watson, to provide the authentication process claims, is not well founded. First, none of the references teaches authentication based on a predicted transaction. It would not be obvious to modify Slater to produce such authentication, because the references do not address the authentication problem.

Enormous public and professional attention is being given currently to the lack of privacy and security of conventional online and offline financial transaction architecture, especially relating the transaction authentication stage. The Examiner's proposal ..."to modify in Slater ..." does not make sense for a number of reasons, among which key ones are as follows: (i) Slater's paramount invention idea is to use debit cards through ATM/POS networks by first submitting the payment request to a merchant – no transaction signature from a financial institution back office ahead of this stage is mentioned in Slater, (ii) Slater's transaction architecture does not include any direct private communication between an account holder and a financial institution back office (a financial server), as such a stage is redundant in Slater's conventional financial transaction architecture.

The Examiner relies on Slater at col. 1, lines 16-40 to teach the prompting limitations in claims 17, 28 and 39. Applicant points out that the cited section of Slater does not describe an authentication process as claimed herein, nor *a priori* the prompting during authentication for a combination of digits from a personal identification code, wherein the combination does not

include all of the personal identification code. In the above citation, Slater describes that even a static PIN is not required to initiate a credit/debit card transaction, which is costly, risky and has disadvantages from a merchant standpoint. Assuming *arguendo* that the PIN is a personal identification code, Slater does not prompt a user during authentication for a combination of less than all digits of a PIN.

In connection with claims 18, 29 and 40, the Examiner relies on Weber at col. 14, lines 12-15 and lines 58-67, col.15, lines 1-10, col.64, lines 31-41, col. 65, lines 27-46, col. 66, line 36 – col. 67, line 39, and col. 103, line 36 – col. 105, line 32. Applicant respectfully disagrees. First, claims 18, 29 and 40 depend from claims 12, 23 and 38 respectively, and are allowable for the same reasons. Furthermore, Weber does not teach use of a transaction signature provided during authentication for a predicted transaction, for authorization of an actual transaction, as required in the claims. Weber does not suggest use of an actual transaction time during authorization, for comparison with timing criteria set up during authentication, as required by the claims herein.

Perhaps the Examiner is confused with Weber's limitation on a particular Terminal ID (TID) to be active in any two concurrent threads (col. 67, lines 15-20), which is partially cured with a data/time tag field (col. 67, lines 40-45). However, this date/time field has nothing to do with the authorization time of a financial transaction defined above; there is no process at the server in Weber, determining whether the actual transaction amount with the predicted transaction amount associated with the transaction signature for the predicted transaction coincide, because Weber does not consider, or define, or use, or imply, or allude to any transaction signature similar to a transaction-specific signature produced during authentication as claimed herein.

As per claims 19, 30, and 41, the Examiner relies on Weber (col. 105, line 38 – col. 106, line 56) to suggest the limitation relating to providing user identification. Applicant respectfully disagrees, and points out that claims 19, 30, and 41 depend from claims 18, 29 and 40, respectively, and are allowable for at least the same reasons.

Claims 20, 31, and 42 recite that the authorization process proceeds without identification of the account holder to the other party to the transaction. The Examiner relies on Slater at col. 5, line 40 to col. 6, line 12, to suggest this limitation. Our analysis revealed that the above reference to Slater does not offer the authorization process operating without identification of the

particular account holder to the party. Moreover, all contemporary transaction systems known to Applicant for online and offline financial transactions, other than ATM transactions, require a card holder to provide some verifiable private and personal information, like personal signature, email address, post address, first and last names, birth date, phone numbers, Social Security number, employment info, and the like. ATM transactions rely on closed networks where a card and a PIN are sufficient for extracting a small amount of money with a usually fixed upper limit amount and a limited number of extractions per day. However, each time a merchant is in a financial transaction loop, some sort of a card holder authentication is required as merchants are liable for fraud with lost or stolen cards. To the best of Applicant's knowledge, the financial transaction architecture offered in the present claims is the first architecture allowing for eliminating merchant requirements to card holders to provide private and personal information. This allows the transactions to proceed, while keeping private information private. In the hands of some merchants, such private information is either misused or sold for profit, or is exposed to theft by online intruders on the merchants' point-of-sales terminals or databases.

Claims 20, 31, and 42 recite that the authorization process proceeds with the identification of the account holder. These claims depend from claims 12, 23 and 38, respectively, and are allowable for the same reasons. The claims emphasize that the transaction architecture can be applied with or without the need for identifying the purchaser with private information to a merchant.

Claims 22, 33 and 44 include limitations similar to those discussed above with respect to claims 16 and 17 and 38 and 39, and are allowable for at least the same reasons.

In connection with claim 23, Applicant points out that it recites an apparatus for executing processes like those discussed above with respect to independent claims 16 and 38. Claim 23 is allowable over the combination applied by the Examiner for at least the same reasons.

Claim 34 depends from claim 23 and is allowable for at least the same reasons, and because of the unique combination recited.

Accordingly, reconsideration of the rejection of claims 16-23, 27-33 and 35-44 as amended is respectfully requested.

Cited Art

It is noted that, although the Examiner confirms in the Action that Applicant has filed Information Disclosure Statements on 25 January 2002, 21 January 2003, 8 May 2003 and 5 April 2003, the Examiner has not provided initialed copies of forms listing the art cited by Applicant in this application. Initialed copies of same are hereby respectfully requested.

CONCLUSION

It is respectfully submitted that this application is now in condition for allowance, and such action is requested.

The Commissioner is hereby authorized to charge any fee determined to be due in connection with this communication, or credit any overpayment, to our Deposit Account No. 50-0869 (AIDT 1000-1).

Respectfully submitted,

Dated: 4 Jan 05

Mark A. Haynes, Reg. No. 30,846

HAYNES BEFFEL & WOLFELD LLP
P.O. Box 366
Half Moon Bay, CA 94019
(650) 712-0340 phone
(650) 712-0263 fax